IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation, Plaintiff and Counterclaim-Defendant, v. INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia corporation, and SYMANTEC CORPORATION, a Delaware corporation, Defendants and Counterclaim-Plaintiffs.	C. A. No. 04-1199 (SLR) **PUBLIC VERSION**

SRI'S OPENING CLAIM CONSTRUCTION BRIEF

FISH & RICHARDSON P.C.
John F. Horvath (#4557)
Kyle Wagner Compton (#4693)
919 N. Market St., Ste. 1100
P.O. Box 1114
Wilmington, DE 19889-1114
Telephone: (302) 652-5070
Facsimile: (302) 652-0607

Howard G. Pollack (CA Bar No. 162897)
Katherine D. Prescott (CA Bar No. 215496)
FISH & RICHARDSON P.C.
500 Arguello St., Ste. 500
Redwood City, CA 94063
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

Attorneys for Plaintiff/Counterclaim Defendant
SRI INTERNATIONAL, INC.

Dated: June 9, 2006

TABLE OF CONTENTS

TABLE OF CONTENTS (cont'd)

TABLE OF AUTHORITIES

Page(s)

Cases

INTRODUCTION

The claims of the patents-in-suit are relatively straightforward, with the majority of the claim terms having clear and unambiguous plain-English meanings. SRI therefore seeks construction of only a handful of terms, in order to improve the jury's understanding of the issues to be resolved. Where it does seek construction, SRI explains the terms' plain and ordinary meanings in light of the entirety of the claims, the specification and the understanding of one of ordinary skill at the relevant time.

Despite the clarity and relative simplicity of the claim language, ISS and Symantec unnecessarily ask the Court to construe numerous terms, many of which have no apparent relevance to any of the disputed issues. For the most part, ISS's and Symantec's proposed constructions are an obvious attempt to limit the claims to the preferred embodiment described in the specification. ISS and Symantec, however, cannot even agree between themselves what characteristics of the preferred embodiment should be imported into the claims. Both are incorrect, however, because no justification exists for reading any of the detailed features of the preferred embodiment into the claims. Such constructions run afoul of well-settled Federal Circuit case law. Furthermore, because all of the patents-in-suit were granted in first office actions of allowance, ISS and Symantec cannot point to amendments or arguments made during prosecution as narrowing the scope of the allowed claims.

In other selected instances, the Defendants go to the opposite extreme: attempting to construe the terms so broadly as to render them meaningless. In these instances, Defendants' transparent motive is to read certain claims and claim limitations directly on the prior art, much of which was cited to the PTO and considered by the Examiner.

Finally, ISS and Symantec cannot even settle on what constructions they propose. On March 17, 2006, the parties submitted their Joint Claim Construction Statement. Subsequently, ISS's and Symantec's non-infringement experts identified still further terms allegedly requiring construction and provided alternative, even more restrictive

definitions of some of the previously identified terms. Because these newly-raised claim constructions from Defendants' experts are untimely, they should be rejected as waived. Even if considered, Defendants' shifting of positions, together with their attempts to read different features of the preferred embodiment into the claims without support in the express claim language, underscore that ISS's and Symantec's proposed constructions are driven by their non-infringement and invalidity contentions, as opposed to the actual language of the claims and other intrinsic evidence. In contrast, SRI's proposed constructions do not materially depart from the plain language of the claims and have ample support in the specification of the patents-in-suit.

I. NATURE AND STAGE OF THE PROCEEDINGS

SRI International, Inc. ("SRI") sued Internet Security Systems, Inc., a Delaware corporation, Internet Security Systems, Inc., a Georgia corporation (collectively, "ISS"), and Symantec Corporation ("Symantec") for infringing U.S. Patent Nos. 6,321,338 ("the '338 patent") [Ex. A], 6,484,203 ("the '203 patent") [Ex. B], 6,711,615 ("the '615 patent") [Ex. C], and 6,708,212 ("the '212 patent") [Ex. D] (collectively, the patents-in-suit).[1] The parties have exchanged expert reports and all discovery relevant to the first trial is complete. The parties submitted their Joint Claim Construction Statement on March 17, 2006. [D.I. 174]. This is SRI's opening brief regarding claim construction. The claim construction hearing is set for August 23, 2006.

II. OVERVIEW

A. The Patents-in-suit

The patents-in-suit relate to computer intrusion detection in large-scale enterprise networks. They share a single omnibus specification,[2] which teaches a computer-automated method of hierarchical event monitoring and analysis within an enterprise

---

1 All referenced exhibits are attached to the Declaration of Kyle Wagner Compton.

2 For the sake of convenience, all citations to the specification will be directed to the '338 patent, regardless of the patent under discussion.

network. This method allows for true real-time detection of suspicious activity, including potential and actual attacks, in the context of complex, distributed enterprise networks.

At the lowest level of the described hierarchical approach, network service monitors[3] are deployed at many places throughout an enterprise network in order to examine network traffic on the fly (as opposed to off-line auditing of log files).[4] [Ex. A at 3:42-44; Fig. 1]. Using a variety of approaches, these network service monitors directly analyze the network traffic data to identify actual attacks, potential attacks, and other suspicious activity. For example, they can compare the monitored network traffic to "signatures" known to be indicative of suspicious activity. [Ex. A at 7:23-8:13]. Alternatively, to detect attacks which do not possess deterministic signatures or to detect previously-unknown (day-zero) attacks, the patents-in-suit also describe the use of statistical detection methods. [Ex. A at 12:46-13:30].

The claims of the '338 patent focus on a particular statistical detection technique involving comparison of statistics of actual, monitored network traffic against statistics of expected traffic. In particular, the '338 patent calls for monitoring network traffic over a relatively long period of time in order to create a "long-term" statistical profile of selected network activity. Then, the patent teaches creating "short-term" statistical profiles over shorter periods of time. Because the short-term statistical profiles should

---

3 As explained below, the patents-in-suit use the more generic term "network monitor" in various claims to sometimes refer to the lowest level of the hierarchy (*see, e.g.*, '203 patent claim 1), but in other contexts use the term to refer to higher-level monitors (*see, e.g.*, '338 patent claim 13). On the other hand, the different term "hierarchical monitor" is always used in the claims to refer only to monitors above the lowest level in the hierarchy that perform functions different from the lowest-level monitors. The nature of the "network monitor" in each claim must, therefore, be determined based on the context of its use.

4 Log files are records of activity at an end-system, *e.g.*, who logged on to a computer, for how long, and what files did they access. Early approaches to intrusion detection involved after-the-fact analysis or auditing of these logs. In contrast, the patents-in-suit are directed to monitoring packets moving through an enterprise network–a much more voluminous source of data–and base the intrusion detection analysis directly on this network traffic.

not vary greatly from the long-term statistical profile, the short-term and long-term profiles can be compared and significant deviations reported as suspicious.

When the network service monitors detect suspicious activity at the level of network traffic analysis, they generate a report of that suspicious activity. The claims of the '203, '212, and '615 patents require a hierarchical monitor (examples of which are referred to in the specification as "domain" and "enterprise" monitors) that automatically receives and integrates these reports, whether they were generated using statistical detection techniques (required by some claims) or some other detection method such as signature matching. This process of automatic integration reduces the volume of information that must be understood by the human network administrator to make security decisions. The claimed hierarchy, therefore, allows for practicable security surveillance of a large enterprise network.

B. Prosecution History

The '338 patent was awarded on November 20, 2001, on an application filed on November 9, 1998. The '203, '615, and '212 patents are all continuations of the '338 patent, and as such, all of the patents-in-suit share a common specification. Each of the patents-in-suit was granted in a first office action of allowance, and accordingly, there is no substantive prosecution history to consider in construing the claims.

III. ANALYSIS

A. Legal Standards

Because this Court is familiar with the legal standards for claim construction, SRI provides only a brief overview of relevant case law for the Court's reference.

Claim construction may be necessary to resolve the meaning of disputed claim terms in order "to clarify and when necessary to explain what the patentee covered by the claims." *United States Surgical Corp. v. Ethicon, Inc.*, 103 F.3d 1554, 1568 (Fed. Cir. 1997). However, claim construction "is not an obligatory exercise in redundancy," and need not be undertaken when the meaning of terms is unambiguous. *Id.* Claim terms

having plain English-language meanings are presumed to "mean what they say." *Johnson Worldwide Assocs., Inc. v. Zebco Corp.*, 175 F.3d 985, 989 (Fed. Cir. 1999). When claim construction is necessary, the starting point of the analysis is always the language of the claims themselves. *Innova/Pure Water, Inc., v. Safari Water Filtration Sys. Inc.*, 381 F.3d 1111, 1116 (Fed. Cir. 2004). The words of the claims, both asserted and unasserted, are examined in their entirety and in the context of the surrounding language. *Vitronics Corp. v. Conceptronics, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996). The claim terms "are generally given their ordinary and customary meaning." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312-13 (Fed. Cir. 2005)(quotations omitted). "The ordinary and customary meaning of a claim term is the meaning that the term would have to a person of ordinary skill in the art at the time of the invention, i.e., as of the effective filing date of that application." *Id.* at 1313.

While claim terms should be construed based upon their use in the claims in which they appear, they may also be construed in light of other claims. As the Federal Circuit has noted, "[t]here is presumed to be a difference in meaning and scope when different words or phrases are used in separate claims. To the extent that the absence of such difference in meaning and scope would make a claim superfluous, the doctrine of claim differentiation states the presumption that the difference between claims is significant." *Comark Communications, Inc. v. Harris Corp.*, 156 F.3d 1182, 1187 (Fed. Cir. 1998) (quoting *Tandon Corp. v. United States Int'l Trade Comm'n*, 831 F.2d 1017, 1023 (Fed. Cir. 1987). Thus, a construction that narrows a claim term in a manner that is explicitly accomplished by limitations that appear in other claims is presumptively unreasonable and wrong. *TurboCare Div. of Demag Delaval Turbomachinery Corp. v. General Electric Co.*, 264 F.3d 1111, 1123 (Fed. Cir. 2001). *See also Phillips*, 415 F.3d at 1315 ("[T]he presence of a dependent claim that adds a particular limitation gives rise to a presumption that the limitation in question is not present in the independent claim.").

After evaluating the claim language itself, the next step of the analysis is the evaluation of "intrinsic evidence" — the specification and the prosecution history.[5] *Vitronics*, 90 F.3d at 1582. The specification is considered "highly relevant to the claim construction analysis" (*Phillips*, 415 F.3d at 1315 (quoting *Vitronics*, 90 F.3d at 1582)) and, while disputed terms should be construed in light of the specification, characteristics of embodiments described in the specification cannot be read as limitations of the claims. *Phillips*, 415 F.3d at 1316 ("[A]lthough the specification often describes very specific embodiments of the invention, we have repeatedly warned against confining the claims to those embodiments."); *TurboCare*, 264 F.3d at 1123 ("[t]here is no basis for reading a limitation from the preferred embodiment into the language of the claim.").

B. Proposed Claim Constructions

The asserted claims of the patents-in-suit share many common terms, and for this reason, SRI's proposed constructions are presented on a term-by-term rather than a patent-by-patent or claim-by-claim basis. The construction of any given claim term is meant to be consistently applied to any of the claims in any of the patents-in-suit in which that claim term appears.

1. Disputed Terms Requiring Construction

SRI believes that only six disputed terms require construction. SRI's proposed constructions of these terms are commensurate with the clear scope of the claims. The constructions proposed by ISS and Symantec, on the other hand, in many cases seek to create or impose limitations that simply are not present in the claim language itself. ISS and Symantec, in an unsupported and piece-meal fashion, each import their own set of some, but not all of the characteristics of the preferred embodiments in an attempt to

[5] Although prosecution history is relevant to claim construction, because each of the patents-in-suit was granted in a first office action of allowance as noted above, there is no prosecution history to consider here.

narrow the scope of the claims. In other instances, the Defendants seek to construe the language so broadly so as to read on the cited prior art.

a. "network monitor" / "monitor"

Claim Term	**"network monitor"** (all patents; multiple claims); **"monitor"** (all patents; multiple claims)
SRI Construction	process or component in a network that can analyze data; depending on the context in specific claims, the network monitor may analyze network traffic data, reports of suspicious network activity or both. Service monitors, domain monitors and enterprise monitors are examples of network monitors
ISS Construction	generic code that can be dynamically configured and reconfigured with reusable modules that define the monitor's inputs, analysis engines and their configurations, response policies and output distribution for its reports
Symantec Construction	software that can be dynamically configured to collect, analyze and respond to suspicious network activity, and that includes one or more analysis engines and a resolver that implements a response policy

The terms "network monitor" and "monitor" appear in multiple claims in each of the patents-in-suit. The parties agree that, when used in this form, these two terms are meant to be interchangeable, and can be construed to have the same meaning.

The plain and ordinary meaning of the term "network monitor" to one of ordinary skill in the art, when read in light of the specifications of the patents-in-suit, is "a process or component in a network that can analyze data." The terms "network" and "monitor" are simple to understand in the context of the patents. And while Defendants will argue that the phrase "network monitor" did not have an established meaning as a term of art, that does not preclude the conclusion that one of skill in the art would have simply taken the words at face value and looked to the remainder of the claim language to further define the subject matter claimed.[6]

[6] The patentee clearly made an effort to make the claims simple to understand through the use of short, descriptive plain-English words. It is ironic that Defendants now attempt to use that against SRI by asserting that the terms must be construed to inherently incorporate a host of specific limitations from the specification.

A plain-English reading of network monitor is supported by the specification as a whole. For example, the specification describes generic network monitors as follows:

> The enterprise 10 includes dynamically deployed network monitors 16a-16f that analyze and respond to network activity and can interoperate to form an analysis hierarchy. The hierarchy includes service monitors 16a-16c, domain monitors 16d-16e, and enterprise monitors 16f.

[Ex. A at 3:32-41].

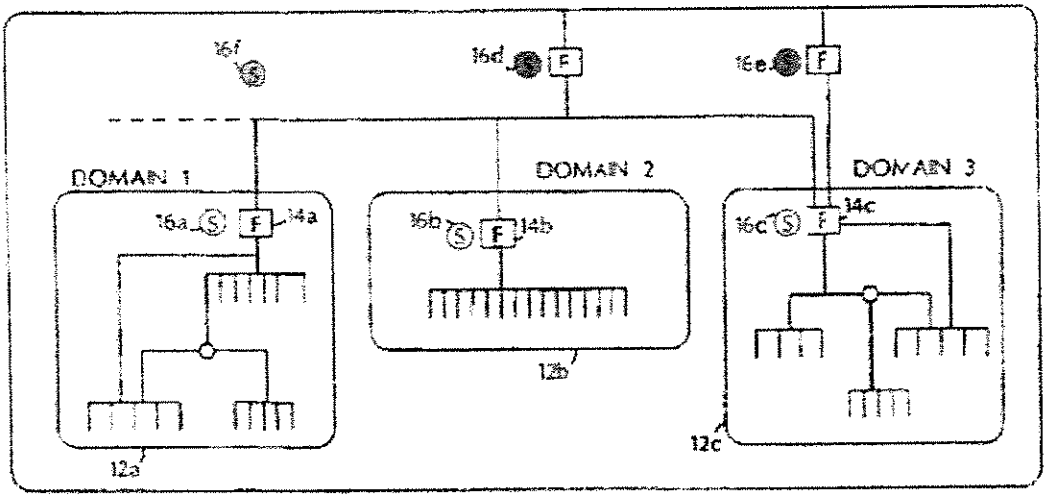

FIG. 1

As the above quote and figure make clear, examples of network monitors (16a-16f) include service monitors (highlighted in yellow), domain monitors (highlighted in red), and enterprise monitors (highlighted in blue). The claims' generic use of the term "monitor" is also apparent from the claims themselves. When it is used, the claims go on to specify the required tasks the monitor must perform, and thereby identify its place in the analysis hierarchy.[7]

---

[7] While it is a general rule that the same term should be construed consistently in all the claims in which it is used, that does not require the term to mean exactly the same thing if it is clear from the context of the claims that variations of meaning are intended. *CAE Screenplates Inc. v. Heinrich Fiedler GmbH & Co. KG*, 224 F.3d 1308, 1317 (Fed. Cir. 2000) ("In some cases, a claim term can be given a different meaning in the various claims of the same patent, when a patent so provides."); *Epcon Gas Systems, Inc. v. Bauer Compressors, Inc.*, 279 F.3d 1022, 1030-1 (Fed. Cir. 2002)(interpreting "substantially" in two different manners as it was used in two

For example, claim 1 of the '203 patent uses the term "monitor" in two different fashions. First, it requires network monitors that include processes or components that analyze network traffic data to detect and generate reports of suspicious activity ("detecting, by the *network monitors*, suspicious network activity based on analysis of network traffic data;" "generating, by the monitors, reports of said suspicious activity"). Claim 1 of the '203 patent also requires a different component—one or more *hierarchical monitors*—that perform the different function of "automatically receiving and integrating the reports of suspicious activity." *See also,* discussion of "hierarchical monitor" below. Thus, the function of the claimed monitors, including what specific type of data they must analyze, is defined contextually by the particular claim element in which "network monitor" or "monitor" is used.

The network monitor constructions proposed by ISS and Symantec, which themselves differ, are flawed because they improperly seek to import limitations from the specification into the claims. *See, e.g., Phillips*, 415 F.3d at 1316 ("[A]lthough the specification often describes very specific embodiments of the invention, we have repeatedly warned against confining the claims to those embodiments."); *TurboCare*, 264 F.3d at 1123 ("[t]here is no basis for reading a limitation from the preferred embodiment into the language of the claim."). Indeed, Defendants' constructions propose that the generic term "network monitor" must not only incorporate many of the limitations of the described "service monitors," but also that the claimed "hierarchical monitors" – which are deployed at different locations in the hierarchy and perform different functions – must incorporate all of the same limitations. For example, both ISS and Symantec propose that network monitor be construed to require "dynamically configured" software or code. While the specification indicates that the various network monitors contain analysis engines that "can be dynamically added, deleted, and modified" [Ex. A at 4:49-50] and

---

different contexts). It is unambiguous in the claims that "network monitor" is intended to be generic and is qualified in any particular claim by the context of its function.

describes a resource object "that configures the monitor" [Ex. A at 4:55-56], nowhere does the language of the claims require the network monitor to be dynamically configurable. Moreover, the meaning of the phrase "dynamic configuration" as used in ISS's and Symantec's proposed constructions is itself ambiguous and confusing and therefore does not help to explain the meaning of the term "network monitor."

ISS, but not Symantec, goes on to propose that "network monitor" also requires "generic code" and "reusable modules." Again, although the specification states that "resource objects may be used by other monitors" [Ex. A at 11:19] and that "the resource object provides a pluggable configuration for tuning the generic code-base" [Ex. A at 11:26-27], neither the specification nor, more importantly, the claims require that the claimed monitors have such features.

Symantec's, but not ISS's[8], construction proposes that network monitors "collect, analyze and respond to suspicious network activity." Claim 1 of the '203 patent, however, contradicts this proposal, specifically requiring that network monitors analyze network traffic data to detect suspicious network activity. Response to the suspicious activity is not mentioned in the claim and, in fact, is the subject of dependent claims.

The claims themselves simply recite a network monitor, and do not by their terms require either a dynamically configurable network monitor composed of generic code or one having reusable modules. SRI's construction is consistent with the plain meaning of the claims. There is no reason to go beyond this plain language of the claims, which go on to include express language describing the specific required tasks of the network monitor. The claims themselves thus completely define the necessary characteristics of each monitor in context. [Ex. E at ¶46; Ex. F at ¶53; Ex. K at 94:12-97:3]. Resort to the specification for additional limitations—under the guise of "construction"— is both

8

REDACTED

factually unwarranted and forbidden as a matter of law. Accordingly, SRI's construction should be adopted.

b. "hierarchical monitor" / "hierarchically higher network monitor"/ "hierarchical event monitoring"

Claim Term	**A. "hierarchical monitor"** ('203, '212, '615; multiple claims); **"hierarchically higher network monitor"** ('338; claim 13)
	B. "hierarchical event monitoring [and analysis]" ('203, '615; multiple claims)
SRI Construction	**A.** process or component in a network that receives reports from at least one lower-level monitor
	B. monitoring events through the use of a hierarchical monitor
ISS Construction	**A.** a network monitor that receives reports as input from one or more network monitors that are at a lower layer in the analysis hierarchy
	B. monitoring and analyzing events through the use of network monitors that are configured to form an analysis hierarchy of two or more layers
Symantec Construction	**A.** a *network monitor* that receives reports from one or more *network monitors* at a lower layer in a hierarchy
	B. Symantec does not believe the term needs construction.

Defendants' overreaching with regard to the "monitor" limitations is even more egregious in the case of the claimed hierarchical monitor. The terms "hierarchical monitor" and "hierarchically higher network monitor" appear in multiple claims in the each of the patents-in-suit. SRI proposes that the terms "hierarchical monitor" and "hierarchically higher network monitor" be construed to mean a "process or component in a network that receives reports from at least one lower-level monitor." This construction is consistent with the usage of these terms in the claims. Claim 1 of the '203 patent, for example, recites "receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors." Similarly, claim 13 of the '338 patent recites "transmitting the event record to a hierarchically higher network monitor." Usage in the specification is also consistent. *See e.g.*, Ex. A at 2:4-6.

ISS's and Symantec's proposed constructions, however, seek to import all the same limitations into the term "hierarchical monitor" that they attempt to import into the

term "network monitor" – and more. As discussed above, these attempts to read limitations of a preferred embodiment into a claim term are improper, and should be rejected. *Phillips*, 415 F.3d at 1316; *TurboCare*, 264 F.3d at 1123.

At present, ISS's position regarding the construction of "hierarchical monitor" is somewhat unclear given the discussion of that term by Stephen E. Smaha, ISS's non-infringement expert. In an attempt to manufacture a non-infringement position, Mr. Smaha suggests for the first time in his expert report that a hierarchical monitor must also itself be capable of sending event reports—rather than just of receiving them. [Ex. G at 17]

REDACTED

Because the Court's scheduling order required the parties to submit their Joint Statement on Claim Construction months ago and states that the parties will be bound by the positions submitted therein absent a showing of good cause [D.I. 52], it is now too late for ISS to adopt the definition discussed in Mr. Smaha's report. The Court should, therefore, expressly reject Mr. Smaha's proposed construction as untimely. To the extent the Court chooses to consider that newly proposed construction on its merits, the construction is incorrect. The claims by their unambiguous terms only require that hierarchical monitors *receive* reports, not that they also *send* them. Mr. Smaha, himself appears to have subsequently recognized this fact.

REDACTED

[Ex. H at 228:1-5].

Symantec's current position regarding the construction of "hierarchical monitor" is also unclear given the report of Jeffery Hansen, Symantec's non-infringement expert. On behalf of Symantec, Dr. Hansen says for the first time that, in addition to the "dynamic configuration" requirement, a hierarchical monitor must also be capable of

REDACTED

[Ex. O at ¶100; *See also* ¶96]. Combining Symantec's construction of network monitor, original construction of hierarchical monitor and the additional limitation proposed by Dr. Hansen yields the following unwieldy and confusing proposed construction of hierarchical monitor:

> software (1) that can be dynamically configured to collect, analyze and respond to suspicious network activity; (2) that can be configured to receive network data packets (e.g., TCP/IP packets) and examine network traffic data in real-time; (3) that includes one or more analysis engines and a resolver that implements a response policy; and (4) that receives reports from other software that can be dynamically configured to collect, analyze and respond to suspicious network activity, and that includes one or more analysis engines and a resolver that implements a response policy.

Again, the Court should reject the additional limitations discussed in Dr. Hansen's report because Symantec failed to timely make such a proposal in accordance with the Court's schedule for submitting claim construction positions. To the extent the Court considers it, however, Dr. Hansen's construction is also incorrect. The claims require only that hierarchical monitors receive *reports*. There is simply no requirement in the claims or the specification that they also receive and themselves examine *network traffic data* – that is what the lower level network monitors analyze, in order to generate the reports that hierarchical monitors receive. Indeed, to require the hierarchical monitors to directly receive and analyze network traffic would frustrate one of the fundamental goals of the invention which is to allow for scalability, by reducing the amount of data that higher levels of the system are required to address and analyze. [Ex. E at ¶31-32

REDACTED

Ex. F at ¶33-34].

By using two different terms in the claims—"network monitor" for the component that looks directly at network traffic and "hierarchical monitor" for the component that receives suspicion reports—the claims clearly establish these components are different. Defendants' constructions would require these different components to

have the same set of functions and all the same limitations Defendants selectively draw in from the specification. As explained above, there is no justification for this position.

The term "hierarchical monitor" is closely related to the phrase "hierarchical event monitoring [and analysis]" which appears in multiple claims of the '203 and '615 patents. SRI and ISS differ in their positions as to what portion of "hierarchical event monitoring [and analysis]" requires construction, while Symantec proposes no construction at all. "Hierarchical event monitoring" should be construed to mean "monitoring events through the use of a hierarchical monitor." This construction captures the plain meaning of the term, as well as the scope of that term as it is used in the claims. The "and analysis" portion of the claims is unambiguous, as well as elaborated upon in further language of claims themselves.

ISS, however, proposes that the entire term "hierarchical event monitoring and analysis" requires construction, and that it should be construed to mean "monitoring and analyzing events through the use of *network monitors* that are configured to form an analysis hierarchy of two or more layers." This construction once again seeks to import the notion that the monitors at the different levels of the hierarchy must all be the identical "network monitors" and, as explained above, this argument should be rejected. ISS is once again also attempting to improperly add the limitation that monitors be "configured" while at the same time providing no explanation of what it means by "configured." That limitation is nowhere to be found in the claims and is itself ambiguous. The surplus language proposed by ISS will only serve to obfuscate an otherwise straightforward construction. For these reasons, Defendants' proposals should be rejected in favor of SRI's construction.

c. "automatically receiving and integrating the reports of suspicious activity"

Claim Term	**"automatically receiving and integrating the reports of suspicious activity"** ('203, '212, '615; multiple claims)
SRI Construction	without user intervention, receiving reports and combining those reports into another functional unit

ISS Construction	automatically receiving and combining the reports of detected suspicious network activity
Symantec Construction	automatically receiving and combining the reports of detected suspicious network activity

The term "automatically receiving and integrating the reports of suspicious activity" appears in multiple claims of the '203, '212, and '615 patents. SRI proposes that the term be construed to mean "without user intervention, receiving reports and combining those reports into another functional unit." Both ISS and Symantec propose that the term be construed to mean "automatically receiving and combining the reports of detected suspicious network activity."

While the proposed constructions bear some facial similarity, SRI's proposed construction provides clearer guidance to a jury and more fully reflects the meaning of the entire phrase. For example, SRI's construction clarifies that the term "automatically" means "without user intervention." *See e.g.*, Ex. I at 125 ("Acting or operating in a manner essentially independent of external influence or control"); Ex. T at 140 ("having the capability of starting, operating, moving, etc., independently"). SRI's construction also clarifies that integration is combination that results in the formation of a new functional unit of information. SRI's construction is consistent with the entirety of the plain and ordinary meaning of the term "integrate." *See e.g.*, Ex. I at 937 ("To make part of a larger unit"); Ex. T at 990 ("to make up, combine, or complete to produce whole or a larger unit, as parts do."); Ex. P at 628 ("To form, coordinate, or blend into a functioning or unified whole: UNITE;" "to incorporate into a larger unit"). The disputed portion of SRI's proposed construction – "combining those reports into another functional unit" – merely adapts the plain and ordinary dictionary definition of "integrate" to the context of the claims. The claimed reports of suspicious activity are the data that get combined to form a whole or larger functional unit. This type of combination is also made clear by the nature of the claimed inventions, which allow multiple levels of automatic analysis,

scaling to large networks and reducing the workload on a human operator. [Ex. E at ¶¶31-32; Ex. F at ¶¶33-34; Ex. K at 194:16-195:3].

ISS's and Symantec's proposed constructions equate "integrate" with "combine", and thus ignore their differing meanings and, in particular, that integration requires formation of a unified whole. Here, Defendants' construction is a transparent attempt to construe the claim so it reads on well-known prior art that provided for the mere collection of data from multiple sensors solely for the purposes of display or central storage. Showing information about security events side by side on a display, for example, or storing it in the same location (which Defendants would characterize as "combining"[9]) is very different from incorporating separate reports into a new functional unit. It is clear from the context of the claims and the specification, that mere "combining" is not what these patents are about—indeed, displaying information to a human operator or allowing manual searches of a database storing suspicion reports is not discussed anywhere in the patents. [*See e.g.*, Ex. K at 328:2-5]. Because SRI's construction provides a clearer and more accurate definition of the claim term which is true to the plain meaning of the words used therein, particularly "integrating," the Court should adopt SRI's construction.

d. "correlating" / "correlates

Claim Term	**"wherein integrating comprises *correlating* intrusion reports reflecting underlying commonalities"** ('203, '212, '615; multiple claims); **"a network monitor that *correlates* activity in the multiple network monitors based on the received event records"** ('338; claim 15)
SRI Construction	combining the reports based on underlying commonalities between them
ISS Construction	determining relationships among the reports of detected suspicious network activity
Symantec Construction	determining relationships among the reports of detected suspicious network activity

[9] SRI does not agree with this characterization.

The expression "wherein integrating comprises *correlating* intrusion reports reflecting underlying commonalities" appears in multiple claims in the '203, '212, and '615 patents, and the expression "a network monitor that correlates activity in the multiple network monitors based on the received event records" appears in claim 15 of the '338 patent. The parties agree that the terms "correlating" and "correlates" as used in these claims can be construed to have the same meaning. SRI proposes that the term "correlating" be construed to mean "combining the reports based on underlying commonalities between them," while both ISS and Symantec propose that this term be construed to mean "determining relationships among the reports of detected suspicious network activity."

SRI's construction reflects the term's context within the claims, whereas ISS's and Symantec's proposed constructions ignore how the term is actually used. For example, SRI incorporates in its construction the claim language specifying that correlation is based upon "underlying commonalities" between reports, whereas the construction proposed by ISS and Symantec fails to specify what types of "relationships" are determined. ISS's and Symantec's proposed constructions also fail to recognize that the claims specify that correlation is a particular type of integration, and thus correlation must result in the combination of the reports into a new functional unit and not just identification of relationships between reports in the abstract. Indeed, according to Defendants' constructions, the claimed correlation might be argued to cover an entirely human driven process rather than what is clearly intended in the patent claims to be computer-automated, thus again attempting to improperly sweep in prior art which has no bearing on these claims. Because SRI's construction conveys the plain meaning of "correlating" in the context of the claim language, SRI's construction should be adopted.

e. "responding . . ." / "invoking countermeasures"

Claim Term	**"responding . . ."** ('338; multiple claims); **"invoking countermeasures"** ('203, '212, '615; multiple claims)
SRI Construction	taking an action in response

ISS Construction	taking an action in response to a suspected attack, including passive responses such as report dissemination to other monitors or administrators, and highly aggressive actions, such as severing a communication channel or the reconfiguration of logging facilities within network components
Symantec Construction	taking an action in response

The parties agree that the terms "responding," as used in the '338 patent, and "invoking countermeasures," as used in the '203, '212, and '615, patents should be similarly construed, and are very close to agreement on that construction. SRI and Symantec agree that those terms should be construed to mean "taking an action in response." ISS agrees with that construction, but proposes to also tack on an open-ended list of possible responses. ISS's additional language is open-ended and neither limits nor clarifies the construction agreed upon by SRI and Symantec. Because ISS's additional verbiage seems superfluous and will not aid the jury in deciding the issues before it, the concise construction agreed upon by SRI and Symantec should be adopted.

f. "building at least one long-term and at least one short-term statistical profile from at least one measure of network packets"

Claim Term	**A. "building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets"** ('338; multiple claims)
	B. "building at least one long-term . . . statistical profile from at least one measure" ('338; multiple claims)
	C. "building . . . at least one short-term statistical profile from at least one measure" ('338; multiple claims)
SRI Construction	**A.** creating at least one statistical description representative of historical network activity, and creating at least one statistical description of recent network activity, where the descriptions are based on one or more measures of network packets
	B. *See above*
	C. *See above*
ISS Construction	**A.** *See below*
	B. automatically generating and updating a description of network activity based on an exponentially aged probability distribution of historically observed values of one or more measures
	C. automatically generating and updating a description of network activity based on an exponentially aged probability distribution of

	recently observed values of one or more measures
Symantec Construction	**A.** *See below*
	B. automatically generating and updating an exponentially aged probability distribution of historically observed activities from at least one measure
	C. automatically generating and updating an exponentially aged probability distribution of recently observed activities from at least one measure

The term "building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets" appears in multiple claims of the '338 patent. The parties differ in their approaches to construing this term. SRI proposes a construction of the term as a whole, while ISS and Symantec propose to construe the term as two constituent parts: "building at least one long-term . . . statistical profile from at least one measure," and "building . . . at least one short-term statistical profile from at least one measure."

SRI proposes that the term be construed in its entirety to mean "creating at least one statistical description representative of historical network activity, and creating at least one statistical description of recent network activity, where the descriptions are based on one or more measures of network packets." This construction conveys the plain meaning of the claim language, and is consistent with the specification. [Ex. A at 1:44-49, 6:38-41, 12:48-52].

ISS and Symantec each propose different constructions that add limitations not found in the claim language. Specifically, they propose construing the terms to require both long-term and short-term profiles that are "exponentially aged probability distributions." Nothing in the claims themselves or the specification requires or suggests such limitations. In fact, the term "probability distribution" does not even appear in the specification. While, the "exponentially aged" characteristic of the statistical profiles is discussed in the specification, it is clearly used to describe a characteristic of a preferred embodiment of the short-term profile. [Ex. A at 6:40-44]. The specification describes the long-term profile being slowly-aged. [Ex. A at 6:51]. Moreover, both the long-term

and short-term profiles are described elsewhere in the specification with reference to "configurable aging parameters" [Ex. A at 6:47] or without any reference to aging at all [Ex. A at 1:44-2:53], thereby confirming that "exponentially aged" is merely a characteristic of a preferred embodiment. Thus the claims cannot properly be read to include the limitations of "exponentially aged" and "probability distribution." *Phillips*, 415 F.3d at 1316. It is also not apparent where Defendants' "generating and updating" language comes from—"building" seems pretty straightforward. Because SRI's proposed construction conveys the plain meaning of the claim terms, while the constructions proposed by ISS and Symantec again attempt to improperly import selected characteristics of a preferred embodiment into the claims, the Court should adopt SRI's proposed construction.

2. Terms That SRI Contends Do Not Require Construction

As discussed above, ISS and Symantec have proposed constructions for numerous additional claim terms from the patents-in-suit. SRI does not believe that these terms require construction because they do not involve technical terminology and/or their plain English-language meaning is clear and unambiguous. Claim construction is used "when necessary to explain what the patentee covered by the claims" and "is not an obligatory exercise in redundancy." *United States Surgical*, 103 F.3d at 1568. However, in the event that the Court finds that construction of these terms would be helpful, SRI proposes constructions based on the plain English-language meaning of the terms as alternatives to the constructions proposed by ISS and Symantec, which are largely based on importing limitations from the specification.

a. "deploying a plurality of network monitors"

Claim Term	**"deploying a plurality of network monitors"** ('203, '212, '615; multiple claims)
SRI Construction	SRI does not believe the term needs construction but, if construed, should be construed to mean locating two or more network monitors so as to allow them to receive data to be monitored and/or to send information.

ISS Construction	installing and configuring two or more network monitors so that together they form an analysis hierarchy defined by the network monitors' inputs and output distribution
Symantec Construction	Installing and configuring two or more *network monitors*

The term "deploying a plurality of network monitors" appears in multiple claims in the '203, '212, and '615 patents. SRI does not believe that this claim language needs to be construed because "deploying" is not a technical word and its plain English-language meaning is unambiguous. However, should the Court determine that construction would be helpful to the jury, one of ordinary skill in the art would understand this expression to mean "locating two or more network monitors so as to allow them to receive data to be monitored and/or to send information." [Ex. E at ¶47; Ex. F at ¶54]. This construction of "deploying a plurality of network monitors" reflects the plain and ordinary meaning of deploying, and is consistent with the remaining claim language that recites the functions performed by the monitors once they are deployed.

In their proposed constructions of "deploying," which differ, ISS and Symantec yet again read limitations into the claims from the specification. For example, both ISS and Symantec improperly construe "deploying" to include "configuring" the network monitors, even though such a limitation is completely absent from the claims.[10] In addition, ISS proposes to construe "deploying" to require forming "an analysis hierarchy defined by the network monitors' inputs and output distribution." However, to the extent that deployment of the monitors in a hierarchical or other fashion is required, it is expressly called out by other portions of the claims. For example, claim 1 of the '203 patent requires a hierarchical monitor, claim 9 of the '203 patent requires placing domain monitors amongst domains of an enterprise, and claim 11 of the '203 patent requires domain monitors to have peer-to-peer relationships.

[10] Of course, neither Defendant explains what they mean by "configuring"— obviously intending to manufacture additional limitations based on this term later to try to avoid infringement.

Besides adding limitations that are nowhere to be found in the claims, the surplus language in ISS's and Symantec's proposed constructions is likely to lead to confusion over what is otherwise an ordinary English phrase that is readily understood. For these reasons, the term "deploying a plurality of network monitors" should either not be construed, or should be construed as proposed by SRI.

b. "service monitor"

Claim Term	**"service monitor"** ('203, '212, '615; multiple claims)
SRI Construction	SRI does not believe the term needs construction but, if construed, should be construed to mean a network monitor that analyzes data from individual components or services.
ISS Construction	a *network monitor* that provides local real-time analysis of network packets handled by a network entity
Symantec Construction	a *network monitor* that provides local real-time analysis of network packets handled by a network entity

The term "service monitor" appears in multiple claims in the '203, '212, and '615 patents. In light of the construction of "monitor" and "network monitor" (discussed above), the meaning of "service monitor" in the context of the claims is clear and SRI does not believe that it needs separate construction. Also, it does not appear that either Defendant is relying on the presence of this term in any claim to support any contention that is not already dependent on their construction of "network monitor" discussed above.

If the Court determines that construction would be helpful, one of skill in the art would understand "service monitor" to mean "a network monitor that analyzes data from individual components or services." SRI's construction of "service monitor" is consistent with the plain English-language meaning of the term and is consistent with the usage in the specification. [Ex. A. at 3:17-24 (describing "local and network services"); 3:38-65, Fig. 1]. ISS and Symantec propose that "service monitor" be construed to mean "a *network monitor* that provides local real-time analysis of network packets handled by a network entity." This proposed construction suggests that "service monitor" should be construed to include the limitations that ISS and Symantec improperly seek to apply to

"*network monitor,*" discussed above. For the same reasons that those limitations cannot be read into "*network monitor*," they cannot be read into the term "service monitor."

ISS's and Symantec's proposed limitations seem to also require that service monitors analyze data from a specific source and in a specific manner. But these are merely features of a preferred embodiment and therefore cannot be read into the claim term "service monitor." *Phillips*, 415 F.3d at 1316. Accordingly, ISS's and Symantec's proposed constructions should be rejected.

c. "domain monitor"

Claim Term	**"domain monitor"** ('203, '212, '615; multiple claims)
SRI Construction	SRI does not believe the term needs construction but, if construed, should be construed to mean a network monitor that analyzes data from a domain.
ISS Construction	A *network monitor* that receives and analyzes intrusion reports disseminated by *service monitors*
Symantec Construction	A *network monitor* that correlates intrusion reports disseminated by *service monitors*

The term "domain monitor" appears in multiple claims in the '203, '212, and '615 patents. Again as "network monitor" and "hierarchical monitor" are already being construed, the meaning of domain monitor in the context of the claims is clear and does not need construction. As with the term service monitors, Defendants also do not appear to be raising any contentions related specifically to this terminology in the claims.

If the Court determines that construction would be helpful, one of skill in the art would understand a "domain monitor" to be "a network monitor that analyzes data from a domain." The specifications of the patents-in-suit describe domain monitors as performing "surveillance over all or part of a domain." [Ex. A at 3:66-67; *See also* Ex. A at 4:2-3]. The defining characteristic of a domain monitor is what it provides surveillance of, not that it necessarily analyzes information from service monitors as suggested by ISS and Symantec. In fact, the specification addresses this very issue by stating that "domain monitors *can* subscribe to service monitors." [Ex. A at 4:7-8 (emphasis added)]. The word "can" emphasizes that it is not necessary that domain

monitors analyze data only from service monitors, but that such an arrangement is a preferred embodiment of domain monitors. Once again ISS and Symantec are attempting to improperly read limitations from the preferred embodiment into the claims.

Moreover, ISS's and Symantec's proposed constructions suggests that "domain monitors" should be construed to include all the limitations that ISS and Symantec improperly seek to apply to "network monitor." For the same reasons discussed above explaining why those limitations cannot be read into the term "network monitor" or "hierarchical monitor," those limitations cannot be read into the term "domain monitor."

Symantec's, and not ISS's, proposed definition would import yet another restriction on the term "domain monitor" – that such a monitor must "*correlate*" reports. As discussed above and is evident from the fact that "correlate" is used in a dependent claim while "integrate" is used in the independent claims, correlation is different than integration. *Cf., e.g.,* claims 1 and 2 of the '203 patent. The claims requiring an a domain monitor require that those monitors perform "receiving and integrating." *See e.g.*, claim 8 of the '203 patent. There is no reason to narrow such claims to specifically require "correlating" where it is not called for by the claim itself.

Consequently, if "domain monitor" is construed, ISS's and Symantec's proposed constructions should be rejected in favor of SRI's proposed construction.

d. "enterprise monitor"

Claim Term	**"enterprise monitor"** ('203, '212, '615; multiple claims)
SRI Construction	SRI does not believe the term needs construction but, if construed, should be construed to mean a network monitor that analyzes data from an enterprise, *i.e.* a collection of domains.
ISS Construction	a *network monitor* that receives and analyzes intrusion reports disseminated by *domain monitors*
Symantec Construction	a *network monitor* that correlates intrusion reports disseminated by *domain monitors*

The term "enterprise monitor" appears in multiple claims in the '203, '212, and '615 patents. Again, SRI does not believe that "enterprise monitor" needs construction because its meaning within the context of the claims and in light of previous

constructions is clear. Also, while ISS and Symantec allege that the claims containing "enterprise monitor" are invalid, SRI does not actually assert infringement of any claims using this term. Nor do Defendants raise any contentions that turn on this phrase.

If the Court determines that construction would be helpful, one of skill in the art would understand an "enterprise monitor" to be "a network monitor that analyzes data from an enterprise, *i.e.*, a collection of domains." SRI's construction of "enterprise monitor" is consistent with the plain English-language meaning of its words, as well as SRI's proposed constructions of the terms "service monitor" and "domain monitor." An enterprise monitor is simply a monitor that analyzes data from an enterprise. The specification explains that an enterprise "includ[es] different domains." [Ex. A at 3:17; *See also* Ex. A at 4:19-20].

Nothing in the claims nor specification requires that an enterprise monitor obtain data specifically in the form of "intrusion reports disseminated by domain monitors," as required by ISS's and Symantec's proposed constructions. Also, it is unclear whether ISS and Symantec use "intrusion report" synonymously with "reports of suspicious activity," a phrase actually used in the claims themselves. Both ISS's and Symantec's proposed constructions of "enterprise monitor" also incorporate the limitations that ISS and Symantec improperly seek to apply to "*network monitor*" and "*hierarchical monitor*." For the same reasons discussed above, those limitations cannot be read into the term "enterprise monitor."

Symantec's further attempt to insert a requirement that enterprise monitor must correlate reports should be rejected for the same reasons as discussed above as to "domain monitor."

In the event the Court decides to construe "enterprise monitor," the Court should adopt SRI's construction because it reflects the plain English-language meaning of this term and is consistent with the language of the claims in light of the specification. The

constructions proposed by ISS and Symantec, which improperly read limitations into the claim terms, should be rejected.

e. "peer-to-peer relationships"

Claim Term	**"peer-to-peer relationships"** ('203, '212, '615; multiple claims)
SRI Construction	SRI does not believe the term needs construction but, if construed, should be construed to mean relationships between two or more entities at the same level in a hierarchy.
ISS Construction	relationships where entities at the same layer in a hierarchy receive reports from one another
Symantec Construction	relationships comprising communication between two or more entities at the same layer in a hierarchy or not in a hierarchy

The term "peer-to-peer relationships" appears in multiple claims in the '203, '212, and '615 patents. SRI does not believe that this term needs construction because its meaning is plain and clear and it does not appear to be determinative of any party's contentions. If the court determines that construction would be helpful, one of skill in the art would understand this term to mean "relationships between two or more entities at the same level in a hierarchy." This construction is consistent with the usage of "peer-to-peer relationships" in the claims and specification of the patents-in-suit. *See e.g.*, Ex. A at 3:24-25 (explaining that relationships are either hierarchical or peer-to-peer).

The construction proposed by ISS reads a limitation into "peer-to-peer relationships" that is not present in the language of the claims. Specifically, ISS's construction would require that entities in peer-to-peer relationships "receive reports from one another." Although this aspect of "peer-to-peer relationships" is described in the specification, it is not a limitation found in the claims. Symantec similarly attempts to construe "peer-to-peer relationships" as "comprising communication," a limitation that again is not present in the claims. Neither the specification nor the claims of the patents-in-suit necessarily requires the term "peer-to-peer relationships" to include communications between peers, whether in the form of receiving reports or otherwise. Thus, ISS's and Symantec's proposed constructions improperly read limitations into the claim term.

f. "selected from one or more" / "selected from"

Claim Term	**"based on analysis of network traffic data *selected from one or more* of the following categories . . ."** ('615; multiple claims); **"based on analysis of network traffic data *selected from* the following categories . . ."** ('203; multiple claims)
SRI Construction	SRI does not believe the phrase needs construction.
ISS Construction	analysis is based on one or more of the following categories
Symantec Construction	analysis is based on one or more of the following categories

The term "based on analysis of network traffic data *selected from one or more* of the following categories . . ." appears in multiple claims of the '615 patent, and the term "based on analysis of network traffic data *selected from* the following categories . . ." appears in multiple claims of the '203 patent. SRI does not believe that these terms require construction because their plain English-language meanings are self evident to lay persons as well as persons skilled in the art. These terms simply "mean what they say." *Johnson Worldwide v. Zebco*, 175 F.3d at 989.

g. "determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity"

Claim Term	**"determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity"** ('338; claims 1, 11, 21, 24, 25)
SRI Construction	SRI does not believe the term needs construction but, if construed, should be construed to mean using the result of the comparison to decide whether the monitored activity is suspicious.
ISS Construction	determining whether the difference between the *short-term statistical profile* and *long-term statistical profile* exceeds a threshold that is empirically determined to indicate suspicious activity based on the historically adaptive deviation between the two profiles, requiring no prior knowledge of suspicious activity
Symantec Construction	determining whether the quantitative difference between the *short-term statistical profile* and the *long-term statistical profile* exceeds a difference which is historically-adaptive for the monitored network, thereby indicating suspicious network activity. This determination requires no prior knowledge of suspicious network activity

The term "determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity" appears in claims 1, 11, 21, 24, and 25 of the '338 patent. SRI does not believe that the term needs construction because its meaning within the context of the claims and in light of constructions previously discussed is clear. If the Court determines that construction would be helpful, one of skill in the art would understand this term to mean "using the result of the comparison to decide whether the monitored activity is suspicious." [Ex. E at ¶147; Ex. F at ¶238].

The construction proposed by SRI is commensurate with the claims, which impose no specific restrictions on how the determining step is performed. By contrast, the various constructions proposed by ISS and Symantec attempt to impose limitations only found in the specification's description of a preferred embodiment, including that the determination be based on whether the difference between the long-term and short-term profiles exceeds an "empirically determined" threshold level of difference that is "historically-adapted" based on past network activity, and that the determination require no prior knowledge of suspicious network activity. While these are characteristics of a preferred embodiment described in the specification, the specification also describes comparisons between long-term and short-term profiles that do not require these limitations. [*See e.g.*, Ex. A at 1:44-2:53]. It is well settled that characteristics of a preferred embodiment described in the specification cannot be properly read into the language of the claims. *Phillips*, 415 F.3d at 1316. Accordingly, the Court should reject the constructions proposed by ISS and Symantec and adopt SRI's proposed construction, which properly reflects the plain meaning of the claim language.

h. "a statistical detection method"

Claim Term	**"a statistical detection method"** ('212, '615; multiple claims)
SRI Construction	SRI does not believe the term needs construction but, if construed, should be construed to mean a method of detecting suspicious network activity by applying one or more statistical functions in the analysis of network traffic data.

ISS Construction	a method that builds a statistical profile of historically observed network traffic activity and a statistical profile of recently observed activity and finds suspicious network activity when the difference between the two exceeds a threshold that is empirically determined to indicate suspicious activity based on the historically adaptive deviation between the two profiles, requiring no prior knowledge of suspicious activity
Symantec Construction	A method of detecting suspicious network activity which comprises building a *long-term statistical profile* and a *short-term statistical profile*. This method requires no prior knowledge of suspicious network activity. This method is not a signature matching detection method or threshold analysis.

The term "a statistical detection method" appears in multiple claims of the '212 and '615 patents. SRI does not believe that this phrase requires construction, as each of its constituent terms has a plain English-language meaning. However, if the Court determines that construction of this term would be helpful, SRI proposes that it be construed to mean "a method of detecting suspicious network activity by applying one or more statistical functions in the analysis of network traffic data."

SRI's proposed construction is consistent with the use of the term "statistical detection method" in the claims, in which the only restriction on the term is that it is a method utilized by a network monitor. [Ex. F at ¶64]. The specification is similarly broad, describing statistical techniques involving categorical approaches [Ex. A at 13:27-30] and analysis of network connection information without requiring that they necessarily use long-term profiles. [Ex. A at 13:31-49; Ex. F at ¶64].

ISS and Symantec propose differing constructions that improperly place limitations on "statistical detection method" which are again not present in the claims. In fact, both construe "statistical detection method" to have the same scope as the limitations of the '338 patent claims, which require building a long-term and a short-term statistical profile and comparing the two to determine suspicious activity, as discussed above. For example, both proposed constructions would require that a "statistical detection method" compare historical or long-term network activity with recent or short-

term network activity and function without any prior knowledge of what constitutes suspicious activity. These are all characteristics of a preferred embodiment described in the specification, and they cannot properly be read into claims which themselves impose no such limitations. *Phillips*, 415 F.3d at 1316.

Further, the fact that the patentee used the different terminology "statistical detection method" in the claims of the '212 patent, which was filed after the '338 patent, rather than the long-term/short-term profile language of the '338 patent, demonstrates that the limitations are not the same. Indeed, if the Examiner believed these limitations were the same, one would have expected a double-patenting rejection or, at the very least, some statement in the prosecution questioning the use of different terminology if the intent was to claim the same subject matter. No such statements were made. Accordingly, if the Court construes "statistical detection method," the Court should reject the improper limitations proposed by ISS and Symantec and adopt SRI's proposed construction, which reflects the plain meaning of the term in light of the specification.

i. "a signature matching detection method"

Claim Term	"a signature matching detection method" ('212; multiple claims)
SRI Construction	SRI does not believe the term needs construction but, if construed, should be construed to mean a method of detecting suspicious network activity by comparing observed network traffic data to known patterns.
ISS Construction	a method of detecting suspicious network activity which comprises comparing observed network traffic data to known patterns or thresholds
Symantec Construction	a method of detecting suspicious activity which comprises comparing observed network traffic data to known patterns or thresholds

The term "a signature matching detection method" appears in claims 2 and 3 of the '212 patent. SRI does not believe this term requires construction, as it can be treated according to its plain meaning to one of skill in the art. However, if the Court believes that the term should be construed, one of ordinary skill in the art would understand the

term to mean "a method of detecting suspicious network activity by comparing observed network traffic data to known patterns."

SRI's proposed construction properly conveys the plain meaning of the claim language and reflects the scope of the claims. Moreover, this construction is supported by the specification, which describes signature analysis as comparing a data stream against known patterns of undesirable activity: "[t]he signature engine 24 maps an event stream against abstract representations of event sequences that are known to indicate undesirable activity. . . . The signature engine scans the event stream for events that represent attempted exploitations of known attacks . . . ." [Ex. A at 7:24-32]. Accordingly, if the Court construes "a signature matching detection method," it should adopt SRI's construction.

ISS and Symantec propose defining signature techniques to also include "comparing observed network traffic to . . . thresholds." This definition is overly broad in that it could even encompass statistical detection methods. For example, in its definition of statistical detection method, ISS requires comparison of the observed difference between profiles to "a *threshold* that is empirically determined." To support their constructions, ISS and Symantec will likely look to the specification and its statement that: "Threshold analysis is a rudimentary, inexpensive signature analysis technique that records the occurrence of specific events and, as the name implies, detects when the number of occurrences of that event surpasses a reasonable count." [Ex. A at 7:46-50]. The described rudimentary threshold analysis, however, is just a specific type of pattern and is much more limited than "comparing observed network traffic data to . . . thresholds." In other words, while thresholds *can be* used in "rudimentary, inexpensive signature analysis," that does not imply that *all* use of thresholds in all contexts involve "signature matching" as suggested by Defendants' proposed constructions. [Ex. K at 483:10-484:1].

Moreover, ISS's current position regarding the construction of "a signature matching detection method" is confused somewhat by the use of the term "suspicious" in the Rebuttal Expert Report of ISS expert Stephen E. Smaha. As discussed above, in the Joint Claim Construction Statement, ISS proposed that a "signature matching detection method" was "a method of detecting suspicious activity."

REDACTED [Ex. J at 6, 8]. "Suspicious" activity, however, includes attacks, possible attacks, and investigation that facilitates future attacks. Also, a pattern or signature match does not imply that an attack has necessarily occurred, but rather indicates that a traffic pattern of interest has occurred. [Ex. K at 64:23-65:23, 486:19-487:1; Ex. H at 209:14-18

Ex. L at 100:2-7

REDACTED

Ex. U at 45:13-17

Further, the plain language of claim 2 of the '212 patent is clearly contrary to Mr. Smaha's position because it is a dependent claim that, in combination with independent claim 1 from which it depends, recites that the network monitors are detecting suspicious network activity using a signature matching detection method. Thus, Defendants' proposed constructions as well as Mr. Smaha's belated attempt to redefine "signature matching detection method" so as to render the claims in which it appears meaningless, should be rejected.

j. "proxy server"

Claim Term	**"proxy server"** (all patents; multiple claims)
SRI Construction	SRI does not believe the term needs construction but, if construed, should be construed to mean a server that mediates communication between a client application, such as a Web browser, and a real server. It handles requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.

ISS Construction	a firewall component that enforces a security policy for a specific application or service
Symantec Construction	a firewall component that enforces a security policy for a specific application or service

The term "proxy server" appears in multiple claims in each of the patents-in-suit. SRI does not believe that the term "proxy server" requires construction because it is commonly used and well understood by persons having ordinary skill in the relevant art. Claim construction is used "when necessary to explain what the patentee covered by the claims" and "is not an obligatory exercise in redundancy." *United States Surgical*, 103 F.3d at 1568. Here, the meaning of "proxy server" is clear. Nor does it appear from any of the various contention interrogatory responses provided in this case that this term is relevant to any validity or infringement position proposed by any party. However, if the Court determines that a construction is helpful, one having ordinary skill in the relevant art would understand the term "proxy server" to mean "a server that mediates communication between a client application, such as a Web browser, and a real server. It handles requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server." [*See e.g.*, Ex. M at SYM_P_0498228 ("A proxy is a program that poses as another")].

ISS and Symantec propose that the term "proxy server" be construed to mean "a firewall component that enforces a security policy for a specific application or service." A fundamental problem with this proposed definition is that it is inconsistent with the use of "proxy server" in the patents-in-suit, which describe proxy servers as distinct from firewalls, rather than as components of firewalls. For example, claim 54 of the '615 patent recites "deploying a plurality of network monitors in the enterprise network, wherein at least one of the network monitors is deployed at a proxy server," while claim 64 of the '615 patent recites "deploying a plurality of network monitors in the enterprise network, wherein at least one of the network monitors is deployed at a firewall." Except for the substitution of the term "firewall" for the term "proxy server," claim 64 is

identical to claim 54. The distinction between the two claims demonstrates that proxy servers are independent of firewalls and require their own independent treatment.

Analysis of the specification of the patents-in-suit leads to the same conclusion. The specification treats firewalls and proxy servers as separate entities: "[n]etwork entities include gateways, routers, firewalls, or proxy servers." [Ex. A at 3:44-45]. By separating the two terms, the specification implies that proxy servers are separate and distinct from firewalls. This contradicts ISS's and Symantec's constructions that "proxy servers" are "firewall components." The testimony of Symantec's own expert is also inconsistent with Defendants' proposed definition. [Ex. N at 75:22-25 (explaining that not all proxy servers are firewalls)]. Accordingly, Defendants' proposed constructions must be rejected and the Court should adopt SRI's proposal.

k. API (Application Programming Interface)

The claim term "API" is used in the phrase "API for encapsulation of monitor functions and integration of third-party tools." *See e.g.*, claims 6 and 17 of the '212 patent; claims 5, 16, and 27 of the '615 patent; and claims 4 and 15 of the '203 patent. API is a commonly used acronym for "application programmers' interface." [Ex. A at 4:58; *See also,* Ex. H at 166:22-23; 167:10-14]. While this term was not identified in the parties' Joint Submission on Claim Construction and SRI does not believe it should require construction, ISS's and Symantec's non-infringement expert reports suggest that they now seek to rely on a newly proposed construction of this term to claim lack of infringement. [Ex. G at 11, 19; Ex. O at ¶¶102, 107]. If construed, SRI proposes that API be explained to mean "a set of routines used to provide for communication of data between application programs or processes." [*See e.g.,* Ex. R at 42 ("The interface between the application software and the application platform, across which all services are provided"); Ex. S at 18 ("A set of routines used by an application program to direct the performance of procedures by the computer's operating system")]. The claims contextualize this generic definition. In the full context, the claim limitation would be

understood to mean a set of routines used to provide for inter-program communication of data which allows for encapsulation of monitor functions and integration of third-party tools into the claimed hierarchy. [Ex. K at 283:13-284:8, 285:15-286:13].

> The specification describes several interfaces related to the claimed API:
>
> "Using this interface specification, third-party modules 28, 30 can communicate with monitors. For example, third-party modules 28 can submit event records to the analysis engines 22, 24 for processing. Additionally, third-party modules 30 may also submit and receive analysis results via the resolver's 20 external interfaces. Thus, third-party modules 28, 30 can incorporate the results from monitors into other surveillance efforts or contribute their results to other monitors 16a-16f."

[Ex. A at 9:11-21; Fig. 2]. Figure 2 also shows that a generic "Monitor API" may be a completely internal interface as well as one that interfaces between a third-party device and a "native" monitor of the system. While the terminology thus could apply to an API between processes within a monitor, the rest of the language of the claim specifies the particular functions of the claimed API—to encapsulate monitor functions and integrate third-party tools.

As discussed above, the claims of the '212, '615, and '203 patents require deploying a plurality of network monitors in an enterprise network. The dependent claims that also require an API specify that, amongst the plurality of network monitors (as opposed to in each and every one the deployed network monitors), there must be an API specifically for the "encapsulation of monitor functions and integration of third-party tools." Therefore the API called out by the claims is a set of routines designed for encapsulating monitoring functions and allowing a third-party tool to communicate or "interface" with the claimed hierarchical monitor. It is this communication that is relevant because, in the context of the claims, the functions of the "plurality of network monitors" are to analyze network traffic and send reports of suspicious activity to the hierarchical monitor. The claimed API allows for "encapsulation" of these functions and

integration of a third-party device to allow that device to perform similar analysis and reporting functions within the claimed hierarchy.

REDACTED

[Ex. G at 11, 19].

[Ex. H at 216:25-217:8]. There is also nothing in the specification's discussion of incorporation of "third-party" data that requires the API and other software that accomplishes the integration be written by a third-party, as opposed to the person supplying the "native" network monitors and hierarchical monitor. The source of these software routines is simply not discussed.

Moreover, the claims require only that there be an API specifically for encapsulation of monitor functions amongst the plurality of network monitors, not that each network monitor must include its own API. The API claims should, therefore, not be artificially limited to some notion of an open-source API resident in each and every network monitor.

3. Constructions the Parties Agree Upon

As set forth in the parties' Joint Claim Construction Statement, the parties agree that "plurality" should be construed to mean "more than one."

SRI does not believe that the terms "virtual private network" or "firewall" need construction, as these terms are commonly used and are well known by persons having ordinary skill in the relevant art. However, if the Court determines that construction is necessary, the parties agree that these terms should be construed as set forth in the parties' Joint Claim Construction Statement.

---

[11] Open-source code is code that is made available to the public such that any third-party would be able to create software that could communicate with the hierarchical monitor.

IV. CONCLUSION

For the foregoing reasons, SRI requests that the Court adopt its proposed constructions of the disputed claim terms of the patents-in-suit.

Dated: June 9, 2006

FISH & RICHARDSON P.C.

By: _____

John F. Horvath (#4557)
Kyle Wagner Compton (#4693)
FISH & RICHARDSON P.C.
919 N. Market St., Ste. 1100
P.O. Box 1114
Wilmington, DE 19889-1114
Telephone: (302) 652-5070
Facsimile: (302) 652-0607

Howard G. Pollack (CA Bar No. 162897)
Katherine D. Prescott (CA Bar No. 215496)
FISH & RICHARDSON P.C.
500 Arguello St., Ste. 500
Redwood City, CA 94063
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

Attorneys for Plaintiff/Counterclaim Defendant
SRI INTERNATIONAL, INC.

CERTIFICATE OF SERVICE

I hereby certify that on June 23, 2006, I electronically filed the **PUBLIC VERSION** of **SRI'S OPENING CLAIM CONSTRUCTION BRIEF** with the Clerk of Court the attached document using CM/ECF which will send electronic notification of such filing(s) to the following Delaware counsel.

Richard L. Horwitz
Potter Anderson & Corroon LLP
Hercules Plaza
1313 North Market Street, 6th Floor
P.O. Box 951
Wilmington, DE 19899

Attorneys for Defendant-Counterclaimant Internet Security Systems, Inc., a Delaware corporation, and Internet Security Systems, Inc., a Georgia corporation

Richard K. Herrmann
Morris James Hitchens & Williams
PNC Bank Center
222 Delaware Avenue, 10th Floor
P.O. Box 2306
Wilmington, DE 19899-2306

Attorneys for Defendant-Counterclaimant Symantec Corporation

/s/ *John F. Horvath*
John F. Horvath

80034097.doc